contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Fundacja Widzialni WidzialniCMS: new CVE

CVE-2026-110468 · record published 9 November 2026

Analysis Report

Anyone running WidzialniCMS before version 2.5 must update — the record scores this 10 on CVSS 4.0, and no login is needed to upload executable files and run code on the server. Update to version 2.5 ...

PREPARED BY	NamiQ	DATE	9 November 2026
FACTS AS OF	9 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 4.0 10.0**	STATUS	Not on CISA's exploited list; exploitation not recorded

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/fundacja-widzialni-widzialnicms-cve-2026-110468

The bottom line

> *Anyone running WidzialniCMS before version 2.5 must update — the record scores this 10 on CVSS 4.0, and no login is needed to upload executable files and run code on the server. Update to version 2.5 first.*

At a glance

Fact	Detail
Product	Fundacja Widzialni WidzialniCMS (CVE-2026-110468)
Severity	Critical: 10 (CVSS 4.0)
Status	A new CVE record, published by CERT-PL on 9 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 9 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	Version 2.5, as stated in the CERT Polska advisory published 9 November 2026.
Who looks first	Any organisation running WidzialniCMS on a version before 2.5. Because no login is required, every internet-facing installation in that version range is at risk regardless of the strength of admin credentials.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run WidzialniCMS on any server?	Nothing to do for this CVE.	Check which version you are running.
Is the version earlier than 2.5?	Nothing to do for this CVE.	Update to version 2.5 — this installation is vulnerable.
Is the installation reachable from the internet or by untrusted users?	Still update, but the immediate risk is lower.	Treat as urgent — no login is needed to exploit this flaw.

What it is

An unauthenticated attacker can upload any file, including executable scripts, to any location on the server through a file upload endpoint. The permission check is handled client-side and can be bypassed; the destination path is not validated. This leads to remote code execution.

Why it matters

Our reading is that a score of 10 on the CVSS 4.0 scale fits: no login is needed, files land wherever the attacker directs, and running arbitrary code on a web server is full compromise. The CERT Polska advisory covers three companion flaws fixed in the same 2.5 release: a second unauthenticated upload path (CVE-2026-110469, also CWE-434), reflected XSS (CVE-2026-112204, CWE-79), and a brute-force bypass on the login page (CVE-2026-112205, CWE-307). These are distinct weaknesses, not variants of this flaw.

What the vendor's advisory says

We read two pages on widzialni.eu and cert.pl. In short:

- CERT Polska's advisory also covers CVE-2026-110469 (CWE-434): a second unauthenticated file upload endpoint (/panel/upload.php) with the same client-side bypass flaw, also leading to remote code execution. Fixed in version 2.5.
- The same advisory covers CVE-2026-112204 (CWE-79): reflected XSS in /index.php, allowing session cookie theft; and CVE-2026-112205 (CWE-307): brute-force login bypass by omitting cookie parameters. Both fixed in version 2.5.

Things people will get wrong

- Locking down the admin panel is sufficient protection. The flaw is in a file upload endpoint and the permission check is client-side, so no admin login is needed. Access controls inside WidzialniCMS do not mitigate it; the fix is updating to version 2.5.
- Only the save_photo.php endpoint needs attention. CERT Polska's advisory describes a second upload flaw (CVE-2026-110469) at a different endpoint, also unauthenticated and also fixed in version 2.5. Both are addressed by updating to 2.5.

How we would triage it

This is our judgement.

Step 1: Find the version you run

- Check the WidzialniCMS admin panel or installation files for the current version number.

- If the version cannot be determined, treat the installation as vulnerable until confirmed otherwise.

Step 2: Restrict access while you prepare the update

- If the installation is internet-facing and an immediate update is not possible, restrict network access to the upload endpoints as a temporary measure.
- CERT Polska's advisory notes the permission check is client-side, so application-level controls within WidzialniCMS are not sufficient on their own.

Step 3: Update to version 2.5

- Apply the update to version 2.5 as supplied by Fundacja Widzialni.
- The CERT Polska advisory states version 2.5 fixes CVE-2026-110468 along with three companion flaws (CVE-2026-110469, CVE-2026-112204, CVE-2026-112205). A single update addresses all four.
- Confirm the installed version after the update completes.

Step 4: Confirm the update and check access controls

- Verify that the installed version shows 2.5 in the WidzialniCMS admin panel.
- Confirm that upload endpoints now reject unauthenticated requests server-side, as the advisory states the previous controls were enforced client-side only.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *We have become aware of a critical security flaw in WidzialniCMS, reference CVE-2026-110468. The vulnerability allows an unauthenticated attacker to upload and execute files on the server; all versions before 2.5 are affected. Version 2.5 is the fixed release, according to the CERT Polska advisory published 9 November 2026. Could you please confirm whether we run WidzialniCMS, which version is installed, and whether version 2.5 has been applied or is scheduled? Please provide written confirmation of the installed version and fix status at your earliest opportunity.*

The weakness behind it

The record classes this as CWE-434.

Likely ATT&CK mapping

MITRE ATT&CK is a public catalogue of the steps attackers take, from getting in to causing damage. No source has mapped this flaw to it yet, so the steps below are our prediction from what the record says the flaw allows. They are not MITRE's, the vendor's or CISA's, and an attacker may do other things.

Steps an attacker would likely take with this flaw

The step, in plain words	Stage of an attack	Why we think so
Exploit Public-Facing Application (T1190): Breaking in through a service that faces the internet, such as a web server, VPN or login page.	Initial Access: getting in	The flaw is in a public-facing web endpoint reachable without authentication; exploiting it would likely be the initial access vector used to gain a foothold on the server.
Command and Scripting Interpreter (T1059): Running commands or scripts on a machine, such as a shell or PowerShell.	Execution: running the attacker's code	Uploading an executable script and accessing it over HTTP would likely result in command execution via the server's scripting interpreter, the typical follow-on to a file upload RCE.

How to use this: ask your IT provider which control or log would show each step, for example whether sign-in attempts from the internet are recorded. If nobody can answer, that is the gap to close first.

MITRE ATT&CK® is a registered trademark of The MITRE Corporation. Technique names are MITRE's.

The sources, in their words

The CVE record:

> *WidzialniCMS is vulnerable to Unrestricted File Upload in the /panel/controllers/save_photo.php endpoint. Due to a client-controlled permission check parameter and insufficient validation of the currentpath parameter, an unauthenticated attacker can upload arbitrary files to any locations on the server, leading to Remote Code Execution. This issue has been fixed in version 2.5.*

Versions of Fundacja Widzialni WidzialniCMS the record lists as affected:

- all versions before 2.5

The record gives no version ranges. Use the vendor's advisory for the affected versions.

Check your own project

If you build software, you can compare what a project declares with this CVE from a terminal. The tool reads requirements files, package.json, Maven, Gradle, Cargo, CMake and Dockerfile files, runs nothing, and only the CVE id leaves your machine. Naming the CVEs needs no key.

```
lattice-scan project . --cve CVE-2026-110468
```

Each row says in-range, outside-range, undetermined or lead, with the file and line. That is evidence about what a manifest declares, not about what runs, and a person decides. The verdicts, the CSV columns and a pipeline recipe are in the guide.

Check the servers you run

The same id can be checked against a host. Run this on the machine itself, not on the laptop that deploys to it: it reads installed packages (dpkg, rpm or apk), snaps, the hardware (maker, model, firmware), the running container images with their operating system and packages, and the kernel version, compares them on the spot, and only the CVE ids leave the machine; the inventory stays on it, in ~/.lattice-scan. Naming the CVEs needs no key. Do it on each server after a deployment, and again when a new entry lands.

```
lattice-scan --cve CVE-2026-110468
```

A match is a candidate for a person to confirm, not a finding. A distribution can fix a CVE under an unchanged version number, so a match is a candidate; on Debian-family hosts the report also shows whether the package's own changelog names the CVE. By default it opens the images your containers are running and reads their operating system and package list; a deep scan (--deep, a few minutes) opens every local image and the Python, Node, Java and Ruby packages inside them; for what an image declares, use the project check on its Dockerfile.

Guide: namiq.io/lattice/guides/choose-your-channel. MCP server (io.namiq/lattice in the MCP registry): namiq.io/lattice. Package: pypi.org/project/lattice-scan, or namiq.io/apt.

What we do not know yet

- The sources do not say how version 2.5 is obtained or whether it is available through an automatic update mechanism or requires direct contact with Fundacja Widzialni.
- The sources do not state whether exploitation occurred before the advisory was published on 9 November 2026.
- The sources do not describe what server-side validation version 2.5 introduces, so it is not possible to verify the fix independently from the version number.
- Exploitation is not recorded. That is not the same as none.

- This is a new record: scores, versions and wording can change in the first days, and they are as at 9 November 2026. We read the vendor pages listed under Sources; nothing here has been tested.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "Likely ATT&CK mapping", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2026-110468: score 10, `CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H` As the CVE record gives it.

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Attack requirements	None	Works against a default deployment.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Vulnerable system: confidentiality	High	Total loss of confidentiality.
Vulnerable system: integrity	High	Total loss of integrity.
Vulnerable system: availability	High	Total loss of availability.
Subsequent systems: confidentiality	High	Total loss of confidentiality.
Subsequent systems: integrity	High	Total loss of integrity.
Subsequent systems: availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
9 November 2026	CVE record published by CERT-PL.

Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe
Internet-facing WidzialniCMS before version 2.5	High	Immediately — no login is needed to exploit

Internal WidzialniCMS before 2.5, reachable by untrusted or unvetted users	High	This week
Internal WidzialniCMS before 2.5, accessible only to trusted staff	Medium	Next patch cycle
WidzialniCMS 2.5 or later, any exposure	None	none for this CVE

Appendix 4. Definition of done

- Every Fundacja Widzialni WidzialniCMS you run is listed, with its version.
- Each is outside the affected list, or the vendor's fix or mitigation is in place.
- The version output or a screenshot is saved with the date.
- Anything not done has an owner and a date.

Sources

- CVE record for CVE-2026-110468: https://www.cve.org/CVERecord?id=CVE-2026-110468
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: widzialni.eu/funkcjonalnosci-widzialni-cms,sd,mg,0,175: https://widzialni.eu/funkcjonalnosci-widzialni-cms,sd,mg,0,175
- Advisory or release notes read: cert.pl/posts/2026/11/CVE-2026-110468/: https://cert.pl/posts/2026/11/CVE-2026-110468/
- Reference in the CVE record: cert.pl: https://cert.pl/posts/2026/11/CVE-2026-110468
- Reference in the CVE record: widzialni.org: https://widzialni.org/funkcjonalnosci-widzialni-cms,sd,mg,0,175